Exhibit 1

Excerpts of SW-SEC00350067

From: Quitugua, Eric [/O=SOLARWINDS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=78D6F037FD3A4708AD1940703AE34840-ERIC QUITUGUA]
Sent: 8/9/2017 8:41:16 PM
To: Brown, Timothy [/o=SolarWinds/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=2c7bcdfd72b7408cb161ab787299e231-Timothy Brown]
Subject: SWI Security Program Assessment
Attachments: SolarWinds Critical Security Controls Assessment workbook - 2017 - CoreIT and MSP.xlsx; SolarWinds Security Program Assessment.xlsx

Flag: Follow up

Here is my assessment of the state of our security program here at SWI with my assessment based on the CIS top 20 critical security controls mapped to the NIST Cybersecurity framework. Monitoring cloud is mostly unobserved/unassessed, so I did not complete a controls assessment workbook on them. My assessment for monitoring cloud is based purely on my observations/interactions with that team over my time here with the company.

solarwinds
Eric Quitugua | Information Security Manager
Office: 512.498.6200

DOCUMENT PRODUCED IN NATIVE FORMAT

DOCUMENT PRODUCED IN NATIVE FORMAT

				Organization		
	Function	Category	CSC Top 20 Controls	CoreIT	MSP	Monitoring Cloud
Governance	Identify	Asset Management	1, 2	2	2	0
		Business Environment	-	0	0	0
		Risk Assessment	-	1	1	0
		Governance	4	2	2	1
	Protect	Risk Management Strategy	-	2	1	1
		Access Control	5, 9, 11, 12, 13, 14, 15, 16	2	2	1
		Awareness and Training	5, 17	1	1	0
		Data Security	1, 2	1	1	1
		Information Protection Processes and Procedures	3, 4, 7, 9, 10, 11, 18, 19	2	1	1
		Maintenance	3, 4, 5, 11, 12	2	2	0
		Protective Technology	5, 6, 7, 8, 11, 13, 14, 16	2	2	1
	Detect	Anomalies and Events	6, 9, 12, 19	2	2	0
		Security Continuous Monitoring	4, 8, 16, 19	3	3	0
		Detection Processes	19	3	3	3
	Respond	Response Planning	19	4	4	4
		Communications	19	4	4	4
		Analysis	6, 19	3	3	3
		Mitigation	4, 19	3	3	3
		Improvements	19, 20	3	3	3
	Recover	Recovery Planning	10	2	2	2
		Improvements	20	2	2	2
		Communications	-	2	2	2

Legend	
Maturity Level	Description
0	There is no evidence of the organization meeting the security control objectives or is unassessed.
1	The organization has an ad-hoc, inconsistent, or reactive approach to meeting the security control objectives
2	The organization has a consistent overall approach to meeting the security control objectives, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.
3	The organization has a documented, detailed approach to meeting the security control objectives, and regularly measures its compliance.
4	The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.
5	The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.